与Openswan建立IPSec VPN

组网需求

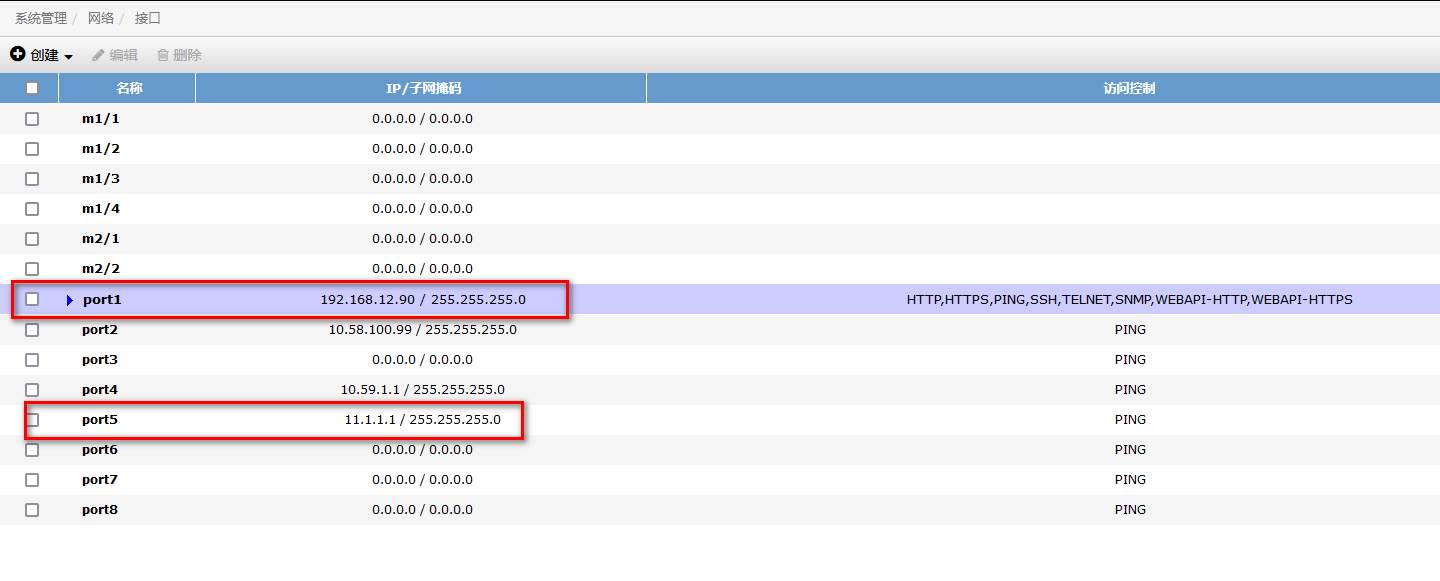
通过IPsec VPN（接口模式）将2个局域网连接起来，实现11.1.0.0/16与12.2.0.0/16两个网段的通信。

网络拓扑

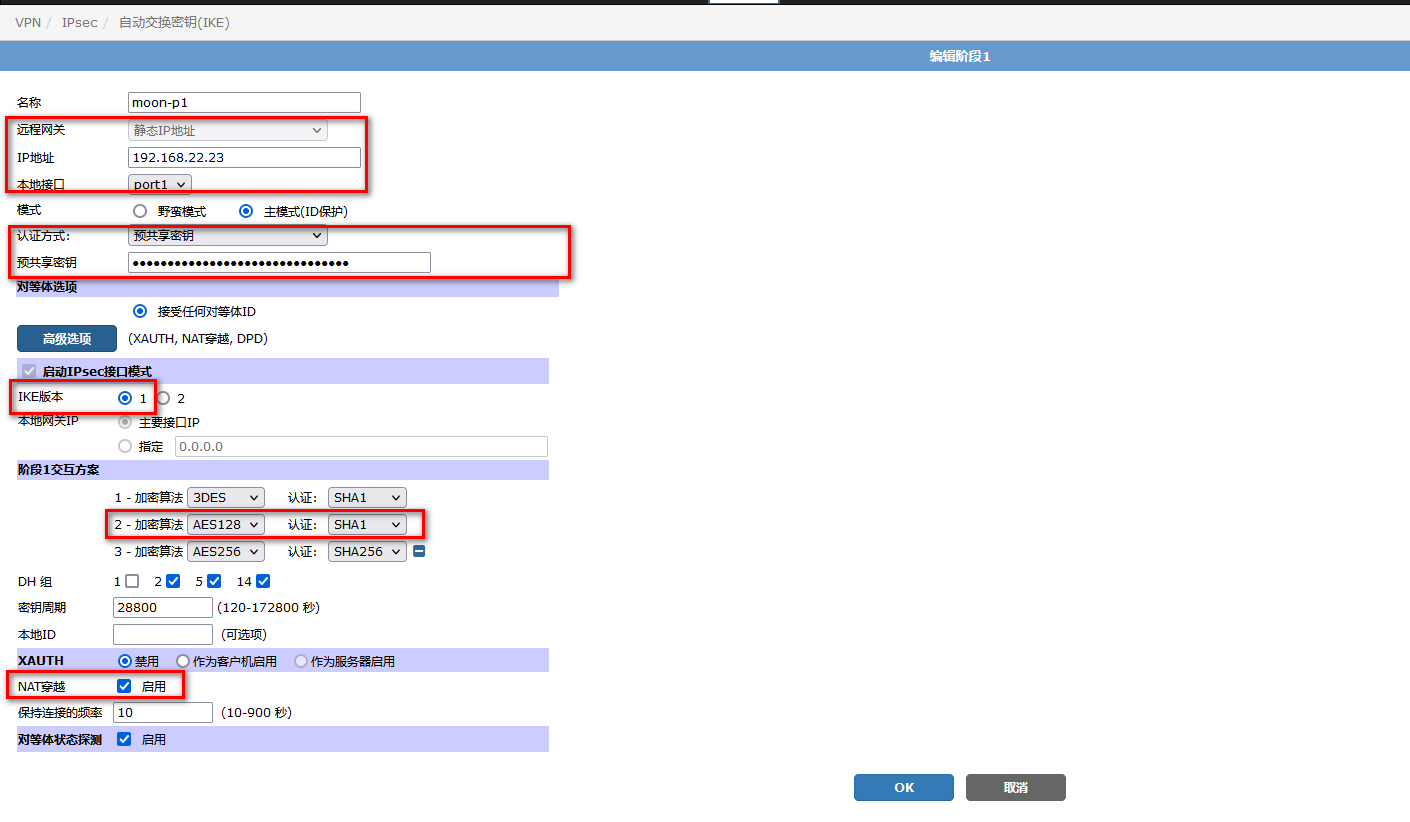
PC1-----(port5:192.168.22.254/24)NGFW(port1:192.168.12.98)---Internet-------(ens192.168.22.23)SPENSWAN(ens256:12.2.1.1/24)----PC2

配置步骤

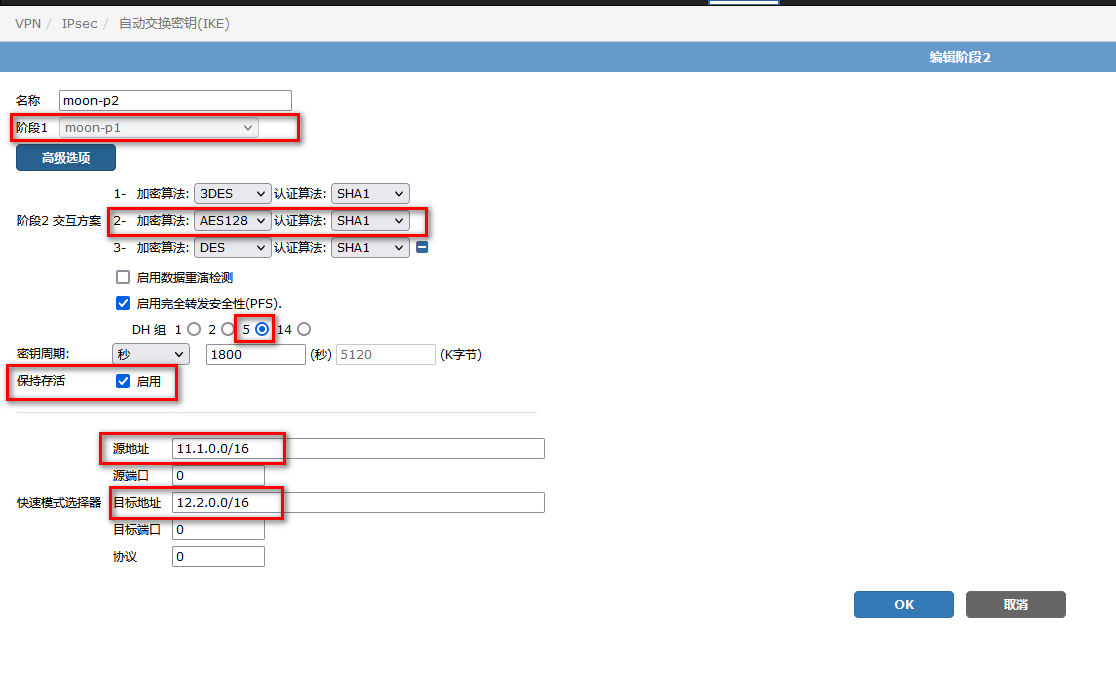
1. 防火墙配置：配置接口



配置IPSEC阶段1



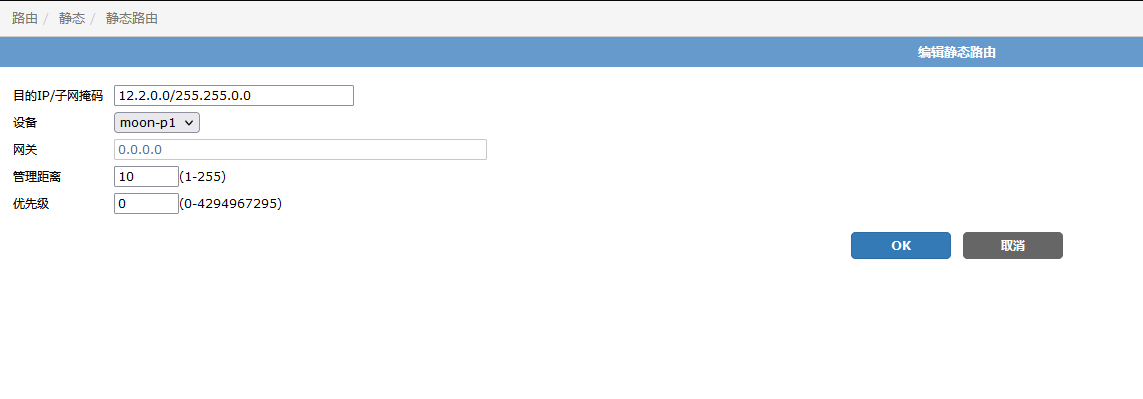
配置IPSec阶段2：



配置策略：

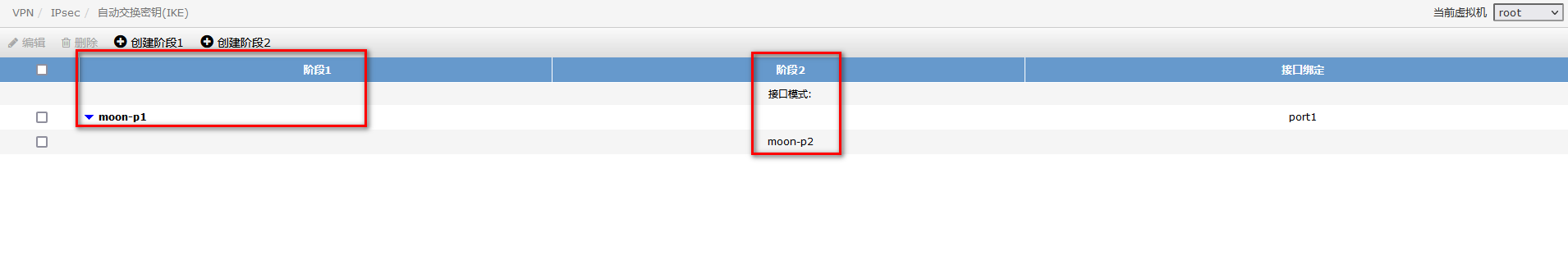


配置路由：

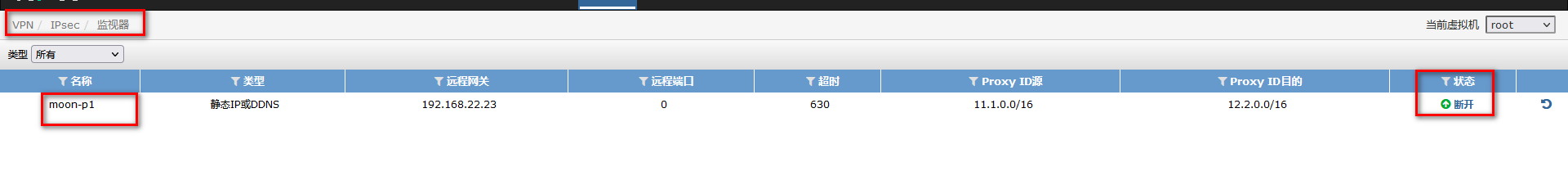


注意：此路由是去程路由，结合实际情况添加其他需要路由

查看：IPSE配置



查看Ipsec状态：



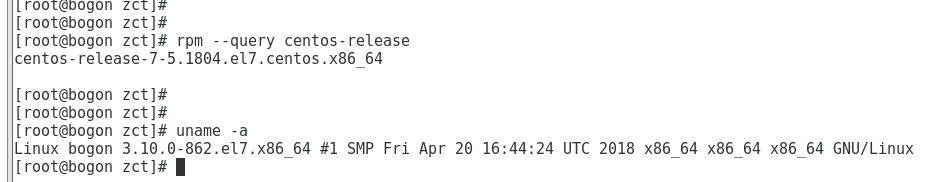
查看IPSEC 日志：



第二部分：

配置OPENSWAN

实验环境：CENTOS



安装openswan

yum install -y openswan

查看openswan安装的配置文件，libreswan即openswan。

# rpm -qc libreswan

/etc/ipsec.conf

/etc/ipsec.d/policies/block

/etc/ipsec.d/policies/clear

/etc/ipsec.d/policies/clear-or-private

/etc/ipsec.d/policies/portexcludes.conf

/etc/ipsec.d/policies/private

/etc/ipsec.d/policies/private-or-clear

/etc/ipsec.secrets

/etc/pam.d/pluto

**开启ipv4转发，关闭ICMP重定向**

cat >> /etc/sysctl.conf << EOF

echo net.ipv4.ip\_forward = 1

EOF

sysctl -a | egrep "ipv4.\*(accept|send)\_redirects" | awk -F "=" '{print$1"= 0"}'

sysctl -a | egrep "ipv4.\*(accept|send)\_redirects" | awk -F "=" '{print$1"= 0"}' >> /etc/sysctl.conf

sysctl -p /etc/sysctl.conf

**关闭SELINUX**

临时关闭：setenforce 0

永久关闭：

#vi /etc/selinux/config

SELINUX=disabled

**关闭防火墙或者开启IPSEC所需的端口UDP 500，UDP4500，ESP**

这里关闭防火墙

systemctl stop firewalld

systemctl disable firewalld

**配置openswan**

在/etc/ipsec.conf中默认包含如下配置，建议将IPsec连接作为单独的文件添加到/etc/ipsec.d/

include /etc/ipsec.d/\*.conf

在/etc/ipsec.secrets中默认包含如下配置，建议将IPsec共享密钥作为单独的文件添加到/etc/ipsec.d/

include /etc/ipsec.d/\*.secrets

**配置IPSEC预共享密钥**

vim /etc/ipsec.d/ipsec.secrets



格式：本地用于连接的IP+空格+远端网关IP+空格+英文冒号+空格+PSK+预共享密钥，冒号的两边都有空格，密钥用英文双引号。

**配置IPSEC连接**

vim /etc/ipsec.d/ipsec.conf



具体含义参考一下：

#ipsec连接名称

conn ipsec1

#phase1

#共享密钥

authby=secret

#start表示ipsec服务启动后会主动发起IPSEC连接;add只表示添加，服务启动不会发起连接,使用ipsec auto --up ipsec名称发起连接

auto=start

#阶段1密钥集

ike=aes128-sha1;modp1536

#ike密钥交换方式

keyexchange=ike

#阶段1生命周期

ikelifetime=86400s

#默认为no主模式，野蛮模式为yes

aggrmode=no

#phase2

#段2传输格式

phase2=esp

#阶段2密钥集

phase2alg=aes128-sha1;modp1536

#关闭压缩

compress=no

#开启PFS

pfs=yes

#阶段2生命周期

salifetime=3600s

#隧道模式

type=tunnel

#本地IP

left=192.168.22.23

#本地子网

leftsubnet=11.1.0.0/16

#远端VPN网关IP

right=100.1.1.2

#远端子网

rightsubnet=192.168.0.0/24

#远端路由按缺省配置

rightnexthop=%defaultroute

#开启dpd检查，每10s发起一次dpd检查，30s没有收到dpd响应，则清楚该ipsec连接

dpddelay=10

dpdtimeout=30

dpdaction=clear

**启动IPSEC服务**

systemctl start ipsec

systemctl enable ipsec

**通过ipsec verify进行配置项校验。如果回显信息全部为OK时，表示配置成功。**

# ipsec verify

Verifying installed system and configuration files

Version check and ipsec on-path [OK]

Libreswan 3.25 (netkey) on 3.10.0-1160.49.1.el7.x86\_64

Checking for IPsec support in kernel [OK]

NETKEY: Testing XFRM related proc values

ICMP default/send\_redirects [OK]

ICMP default/accept\_redirects [OK]

XFRM larval drop [OK]

Pluto ipsec.conf syntax [OK]

Two or more interfaces found, checking IP forwarding [OK]

Checking rp\_filter [OK]

Checking that pluto is running [OK]

Pluto listening for IKE on udp 500 [OK]

Pluto listening for IKE/NAT-T on udp 4500 [OK]

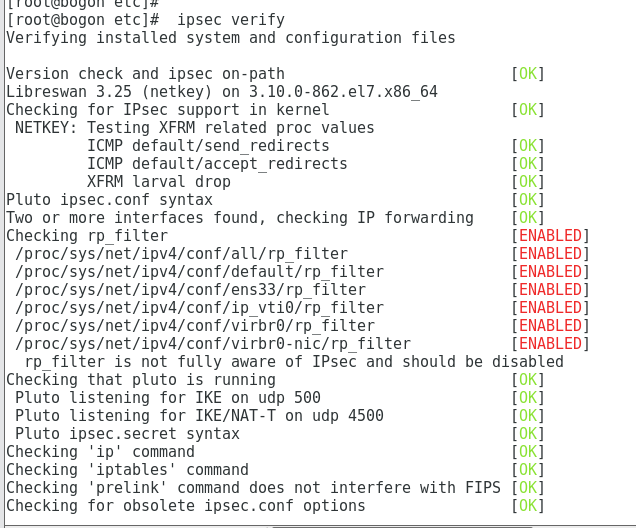
Pluto ipsec.secret syntax [OK]

Checking 'ip' command [OK]

Checking 'iptables' command [OK]

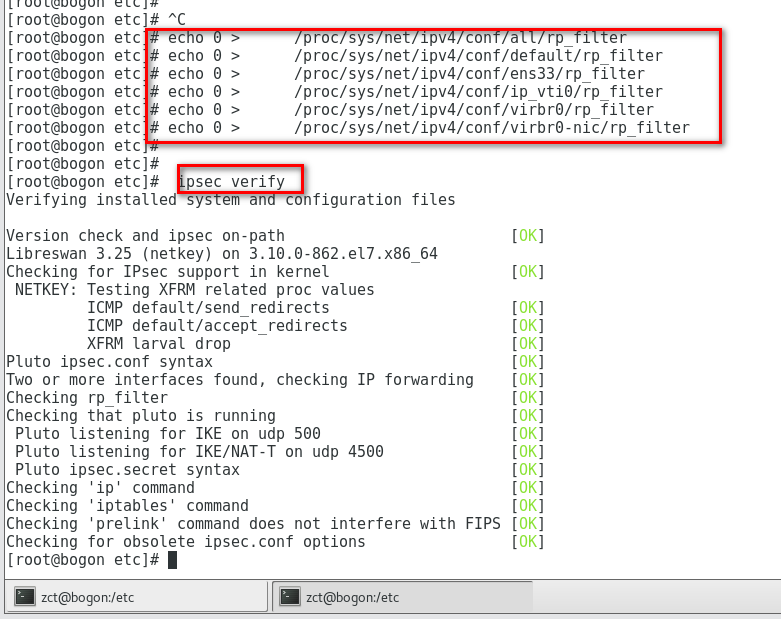
Checking 'prelink' command does not interfere with FIPS [OK]

Checking for obsolete ipsec.conf options [OK]



如遇到上述报错：

一下命令修改：



查看状态：

[root@bogon etc]# ipsec status

000 using kernel interface: netkey

000 interface lo/lo ::1@500

000 interface lo/lo 127.0.0.1@4500

000 interface lo/lo 127.0.0.1@500

000 interface ens33/ens33 192.168.22.23@4500

000 interface ens33/ens33 192.168.22.23@500

000 interface virbr0/virbr0 192.168.122.1@4500

000 interface virbr0/virbr0 192.168.122.1@500

000

000

000 fips mode=disabled;

000 SElinux=enabled

000 seccomp=disabled

000

000 config setup options:

000

000 configdir=/etc, configfile=/etc/ipsec.conf, secrets=/etc/ipsec.secrets, ipsecdir=/etc/ipsec.d

000 nssdir=/etc/ipsec.d, dumpdir=/run/pluto, statsbin=unset

000 dnssec-rootkey-file=/var/lib/unbound/root.key, dnssec-trusted=<unset>

000 sbindir=/usr/sbin, libexecdir=/usr/libexec/ipsec

000 pluto\_version=3.25, pluto\_vendorid=OE-Libreswan-3.25

000 nhelpers=-1, uniqueids=yes, dnssec-enable=yes, perpeerlog=no, logappend=yes, logip=yes, shuntlifetime=900s, xfrmlifetime=300s

000 ddos-cookies-threshold=50000, ddos-max-halfopen=25000, ddos-mode=auto

000 ikeport=500, ikebuf=0, msg\_errqueue=yes, strictcrlpolicy=no, crlcheckinterval=0, listen=<any>, nflog-all=0

000 ocsp-enable=no, ocsp-strict=no, ocsp-timeout=2, ocsp-uri=<unset>

000 ocsp-trust-name=<unset>

000 ocsp-cache-size=1000, ocsp-cache-min-age=3600, ocsp-cache-max-age=86400, ocsp-method=get

000 secctx-attr-type=32001

000 debug:

000

000 nat-traversal=yes, keep-alive=20, nat-ikeport=4500

000 virtual-private (%priv):

000 - allowed subnets: 10.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12, 25.0.0.0/8, 100.64.0.0/10, fd00::/8, fe80::/10

000

000 ESP algorithms supported:

000

000 algorithm ESP encrypt: id=3, name=ESP\_3DES, ivlen=8, keysizemin=192, keysizemax=192

000 algorithm ESP encrypt: id=6, name=ESP\_CAST, ivlen=8, keysizemin=128, keysizemax=128

000 algorithm ESP encrypt: id=11, name=ESP\_NULL, ivlen=0, keysizemin=0, keysizemax=0

000 algorithm ESP encrypt: id=12, name=ESP\_AES, ivlen=8, keysizemin=128, keysizemax=256

000 algorithm ESP encrypt: id=13, name=ESP\_AES\_CTR, ivlen=8, keysizemin=128, keysizemax=256

000 algorithm ESP encrypt: id=14, name=ESP\_AES\_CCM\_A, ivlen=8, keysizemin=128, keysizemax=256

000 algorithm ESP encrypt: id=15, name=ESP\_AES\_CCM\_B, ivlen=8, keysizemin=128, keysizemax=256

000 algorithm ESP encrypt: id=16, name=ESP\_AES\_CCM\_C, ivlen=8, keysizemin=128, keysizemax=256

000 algorithm ESP encrypt: id=18, name=ESP\_AES\_GCM\_A, ivlen=8, keysizemin=128, keysizemax=256

000 algorithm ESP encrypt: id=19, name=ESP\_AES\_GCM\_B, ivlen=8, keysizemin=128, keysizemax=256

000 algorithm ESP encrypt: id=20, name=ESP\_AES\_GCM\_C, ivlen=8, keysizemin=128, keysizemax=256

000 algorithm ESP encrypt: id=22, name=ESP\_CAMELLIA, ivlen=8, keysizemin=128, keysizemax=256

000 algorithm ESP encrypt: id=23, name=ESP\_NULL\_AUTH\_AES\_GMAC, ivlen=8, keysizemin=128, keysizemax=256

000 algorithm ESP encrypt: id=252, name=ESP\_SERPENT, ivlen=8, keysizemin=128, keysizemax=256

000 algorithm ESP encrypt: id=253, name=ESP\_TWOFISH, ivlen=8, keysizemin=128, keysizemax=256

000 algorithm AH/ESP auth: id=1, name=AUTH\_ALGORITHM\_HMAC\_MD5, keysizemin=128, keysizemax=128

000 algorithm AH/ESP auth: id=2, name=AUTH\_ALGORITHM\_HMAC\_SHA1, keysizemin=160, keysizemax=160

000 algorithm AH/ESP auth: id=5, name=AUTH\_ALGORITHM\_HMAC\_SHA2\_256, keysizemin=256, keysizemax=256

000 algorithm AH/ESP auth: id=6, name=AUTH\_ALGORITHM\_HMAC\_SHA2\_384, keysizemin=384, keysizemax=384

000 algorithm AH/ESP auth: id=7, name=AUTH\_ALGORITHM\_HMAC\_SHA2\_512, keysizemin=512, keysizemax=512

000 algorithm AH/ESP auth: id=8, name=AUTH\_ALGORITHM\_HMAC\_RIPEMD, keysizemin=160, keysizemax=160

000 algorithm AH/ESP auth: id=9, name=AUTH\_ALGORITHM\_AES\_XCBC, keysizemin=128, keysizemax=128

000 algorithm AH/ESP auth: id=250, name=AUTH\_ALGORITHM\_AES\_CMAC\_96, keysizemin=128, keysizemax=128

000 algorithm AH/ESP auth: id=251, name=AUTH\_ALGORITHM\_NULL\_KAME, keysizemin=0, keysizemax=0

000

000 IKE algorithms supported:

000

000 algorithm IKE encrypt: v1id=5, v1name=OAKLEY\_3DES\_CBC, v2id=3, v2name=3DES, blocksize=8, keydeflen=192

000 algorithm IKE encrypt: v1id=8, v1name=OAKLEY\_CAMELLIA\_CBC, v2id=23, v2name=CAMELLIA\_CBC, blocksize=16, keydeflen=128

000 algorithm IKE encrypt: v1id=-1, v1name=n/a, v2id=20, v2name=AES\_GCM\_C, blocksize=16, keydeflen=128

000 algorithm IKE encrypt: v1id=-1, v1name=n/a, v2id=19, v2name=AES\_GCM\_B, blocksize=16, keydeflen=128

000 algorithm IKE encrypt: v1id=-1, v1name=n/a, v2id=18, v2name=AES\_GCM\_A, blocksize=16, keydeflen=128

000 algorithm IKE encrypt: v1id=13, v1name=OAKLEY\_AES\_CTR, v2id=13, v2name=AES\_CTR, blocksize=16, keydeflen=128

000 algorithm IKE encrypt: v1id=7, v1name=OAKLEY\_AES\_CBC, v2id=12, v2name=AES\_CBC, blocksize=16, keydeflen=128

000 algorithm IKE encrypt: v1id=65004, v1name=OAKLEY\_SERPENT\_CBC, v2id=65004, v2name=SERPENT\_CBC, blocksize=16, keydeflen=128

000 algorithm IKE encrypt: v1id=65005, v1name=OAKLEY\_TWOFISH\_CBC, v2id=65005, v2name=TWOFISH\_CBC, blocksize=16, keydeflen=128

000 algorithm IKE encrypt: v1id=65289, v1name=OAKLEY\_TWOFISH\_CBC\_SSH, v2id=65289, v2name=TWOFISH\_CBC\_SSH, blocksize=16, keydeflen=128

000 algorithm IKE PRF: name=HMAC\_MD5, hashlen=16

000 algorithm IKE PRF: name=HMAC\_SHA1, hashlen=20

000 algorithm IKE PRF: name=HMAC\_SHA2\_256, hashlen=32

000 algorithm IKE PRF: name=HMAC\_SHA2\_384, hashlen=48

000 algorithm IKE PRF: name=HMAC\_SHA2\_512, hashlen=64

000 algorithm IKE PRF: name=AES\_XCBC, hashlen=16

000 algorithm IKE DH Key Exchange: name=MODP1024, bits=1024

000 algorithm IKE DH Key Exchange: name=MODP1536, bits=1536

000 algorithm IKE DH Key Exchange: name=MODP2048, bits=2048

000 algorithm IKE DH Key Exchange: name=MODP3072, bits=3072

000 algorithm IKE DH Key Exchange: name=MODP4096, bits=4096

000 algorithm IKE DH Key Exchange: name=MODP6144, bits=6144

000 algorithm IKE DH Key Exchange: name=MODP8192, bits=8192

000 algorithm IKE DH Key Exchange: name=DH19, bits=512

000 algorithm IKE DH Key Exchange: name=DH20, bits=768

000 algorithm IKE DH Key Exchange: name=DH21, bits=1056

000 algorithm IKE DH Key Exchange: name=DH22, bits=1024

000 algorithm IKE DH Key Exchange: name=DH23, bits=2048

000 algorithm IKE DH Key Exchange: name=DH24, bits=2048

000

000 stats db\_ops: {curr\_cnt, total\_cnt, maxsz} :context={0,6,64} trans={0,6,6936} attrs={0,6,4624}

000

000 Connection list:

000

000 "ipsec1": 12.2.0.0/16===192.168.22.23<192.168.22.23>...192.168.12.90<192.168.12.90>===11.1.0.0/16; erouted; eroute owner: #18

000 "ipsec1": oriented; my\_ip=unset; their\_ip=unset; my\_updown=ipsec \_updown;

000 "ipsec1": xauth us:none, xauth them:none, my\_username=[any]; their\_username=[any]

000 "ipsec1": our auth:secret, their auth:secret

000 "ipsec1": modecfg info: us:none, them:none, modecfg policy:push, dns:unset, domains:unset, banner:unset, cat:unset;

000 "ipsec1": labeled\_ipsec:no;

000 "ipsec1": policy\_label:unset;

000 "ipsec1": ike\_life: 86400s; ipsec\_life: 3600s; replay\_window: 32; rekey\_margin: 540s; rekey\_fuzz: 100%; keyingtries: 0;

000 "ipsec1": retransmit-interval: 500ms; retransmit-timeout: 60s;

000 "ipsec1": initial-contact:no; cisco-unity:no; fake-strongswan:no; send-vendorid:no; send-no-esp-tfc:no;

000 "ipsec1": policy: PSK+ENCRYPT+TUNNEL+PFS+UP+IKEV1\_ALLOW+IKEV2\_ALLOW+SAREF\_TRACK+IKE\_FRAG\_ALLOW+ESN\_NO;

000 "ipsec1": conn\_prio: 16,16; interface: ens33; metric: 0; mtu: unset; sa\_prio:auto; sa\_tfc:none;

000 "ipsec1": nflog-group: unset; mark: unset; vti-iface:unset; vti-routing:no; vti-shared:no; nic-offload:auto;

000 "ipsec1": our idtype: ID\_IPV4\_ADDR; our id=192.168.22.23; their idtype: ID\_IPV4\_ADDR; their id=192.168.12.90

000 "ipsec1": dpd: action:clear; delay:10; timeout:30; nat-t: encaps:auto; nat\_keepalive:yes; ikev1\_natt:both

000 "ipsec1": newest ISAKMP SA: #17; newest IPsec SA: #18;

000 "ipsec1": IKE algorithms: AES\_CBC\_128-HMAC\_SHA1-MODP1536

000 "ipsec1": IKE algorithm newest: AES\_CBC\_128-HMAC\_SHA1-MODP1536

000 "ipsec1": ESP algorithms: AES\_CBC\_128-HMAC\_SHA1\_96-MODP1536

000 "ipsec1": ESP algorithm newest: AES\_CBC\_128-HMAC\_SHA1\_96; pfsgroup=MODP1536

000

000 Total IPsec connections: loaded 1, active 1

000

000 State Information: DDoS cookies not required, Accepting new IKE connections

000 IKE SAs: total(1), half-open(0), open(0), authenticated(1), anonymous(0)

000 IPsec SAs: total(2), authenticated(2), anonymous(0)

000

000 #10: "ipsec1":500 STATE\_QUICK\_I2 (sent QI2, IPsec SA established); EVENT\_SA\_REPLACE in 464s; isakmp#9; idle; import:admin initiate

000 #10: "ipsec1" esp.d736092d@192.168.12.90 esp.7adf6cb6@192.168.22.23 tun.0@192.168.12.90 tun.0@192.168.22.23 ref=0 refhim=0 Traffic: ESPin=0B ESPout=0B! ESPmax=4194303B

000 #17: "ipsec1":500 STATE\_MAIN\_I4 (ISAKMP SA established); EVENT\_SA\_REPLACE in 84869s; newest ISAKMP; lastdpd=1s(seq in:0 out:0); idle; import:admin initiate

000 #18: "ipsec1":500 STATE\_QUICK\_I2 (sent QI2, IPsec SA established); EVENT\_SA\_REPLACE in 2060s; newest IPSEC; eroute owner; isakmp#17; idle; import:admin initiate

000 #18: "ipsec1" esp.d7360930@192.168.12.90 esp.bec131a3@192.168.22.23 tun.0@192.168.12.90 tun.0@192.168.22.23 ref=0 refhim=0 Traffic: ESPin=0B ESPout=0B! ESPmax=4194303B

000

000 Bare Shunt list:

000

[root@bogon etc]#

业务测试：

从11.1.1.2 ping 12.2.1.1 可ping通

从中间设备抓ESP报文：

